Les événements de liste verte de la stratégie de corrélation FMC nécessitent l'activation de la stratégie de découverte du réseau

Table des matières

Problème

Lors de la configuration des stratégies de corrélation avec les listes d'autorisation sur Cisco Secure Firewall Management Center (FMC), il est important de noter que Allow List Events et Allow List Violations ne sont pas générés sauf si la stratégie de découverte de réseau est configurée pour l'adresse IP du réseau cible. Sans cette configuration, aucun événement n'apparaît sous Analyse > Corrélation > Autoriser les événements de liste et Analyse > Corrélation > Autoriser les violations de liste.

Au cours d'essais en laboratoire, ces comportements ont été observés :

- Les événements de corrélation sont générés correctement pour le réseau cible configuré.
- Aucun événement Allow List ou Allow List Violations sont générés lorsque l'hôte réseau cible n'est plus conforme.

Environnement

- Cisco Firepower Threat Defense (FTD) géré par Secure Firewall Management Center (FMC)
- Stratégie de corrélation configurée avec une liste autorisée ciblant des adresses IP spécifiques
- Liste d'autorisation configurée pour autoriser une application Web, une application ou un protocole spécifique

Résolution

Après des tests approfondis en laboratoire et une consultation avec l'équipe de développement, il a été confirmé que la stratégie de découverte de réseau doit être activée comme condition préalable à la génération de Allow List Events et de Allow List Violations.

La résolution comprend les étapes suivantes :

Étape 1: Activer la stratégie de découverte de réseau

Accédez à Policies > Network Discovery dans l'interface FMC et créez une règle si aucune n'existe.

Étape 2: Configurer la règle de détection de réseau

Configurez la règle de détection de réseau avec les paramètres réseau source appropriés :

- Spécifiez le réseau source en tant que plage réseau interne.
- Vous pouvez également utiliser tous les réseaux (0.0.0.0/0) pour surveiller toutes les sources de trafic.
- Assurez-vous que la règle couvre les réseaux à partir desquels vous prévoyez de générer des événements de liste verte.

Étape 3: Activer les règles de stratégie de corrélation

Vérifiez que les règles de stratégie de corrélation sont actives et non désactivées.

Étape 4: Vérifier la génération des événements de liste verte

Après avoir activé la détection de réseau et activé les règles de stratégie de corrélation :

1.- Accéder aux sites Web à partir du réseau cible configuré à l'aide d'un navigateur (rendant l'hôte non conforme).

2.- Surveiller l'analyse > Corrélation > Autoriser les événements de liste et Analyse > Corrélation > Autoriser les violations de liste pour la génération d'événements.

3.- Vérifiez que les événements sont renseignés lorsque l'hôte n'est pas conforme.

Les tests en laboratoire ont confirmé qu'une fois que la découverte de réseau est activée, les événements Allow List et les violations de la liste Allow sont générés avec succès pour un hôte non conforme.

Motif

La cause principale est que la stratégie de découverte de réseau est une condition préalable obligatoire pour générer des événements de liste d'autorisation dans les stratégies de corrélation FMC. Sans une stratégie de découverte de réseau active, le système ne peut pas évaluer correctement la conformité de l'hôte par rapport à la liste verte configurée, ce qui a pour conséquence qu'aucun événement de liste verte n'est généré lorsque l'hôte du réseau cible devient non conforme.

Autres informations utiles

- Documentation des listes de conformité de corrélation Cisco FMC
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.